Errata: HPL-2004-170 (R.2), Formal Aspects of Computing, 18: 495- (2006) and Electronic Notes in Theoretical Computer Science, 172: 545- (2007)

Matthew Collinson, David Pym, Chris Tofts
Trusted Systems Laboratory
HP Laboratories Bristol
HPL-2007-153
September 18, 2007*

errata, hpl-2004-170 (R.2), logic, concurrency, resources, processes, modelling, parallel

We present a correction for an error that occurs in the following papers:

- HPL-2004-170 (R.2);
- *Formal Aspects of Computing* (2006)18: 495-517; and
- *Electronic Notes in Theoretical Computer Science* 172: 545-587, 2007.

At first sight, the error appears to be simply a misplaced quantifier in the definition of bisimulation. We explain, however, that the error and its correction reveal a subtle interaction between the substructural connectives of **MBI** and the resource-process calculus **SCRP**.

We begin with a specific example which illustrates the error. We include also the known typographical errors.

* Internal Accession Date Only

Approved for External Publication

ERRATA: HPL-2004-170R2, *FORMAL ASPECTS OF COMPUTING* (2006) 18:495–517, AND *ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE* 172, 545–587, 2007

MATTHEW COLLINSON, DAVID PYM, AND CHRIS TOFTS

Abstract. We present a correction for an error that occurs in the following papers:

- HPL-2004-170R2;
- *Formal Aspects of Computing* (2006) 18:495–517; and
- *Electronic Notes in Theoretical Computer Science* 172, 545–587, 2007.

At first sight, the error appears to be simply a misplaced quantifier in the definition of bisimulation. We explain, however, that the error and its correction reveal a subtle interaction between the substructural connectives of **MBI** and the resource–process calculus **SCRP**.

We begin with a specific example which illustrates the error. We include also the known typographical errors.

1. Example

We begin with an example that illustrates an error in the definition of bisimulation used in [PT06].

We start with the resource monoid $(\mathbb{N}, +, 0, =)$ and the action monoid

$$Act = \{i^p z^q \mid p, q \in \mathbb{N}\}$$

generated freely from two primitive actions z and i. Note that, for simplicity, we take here just individual resources rather than sets of resources. This is an inessential change with no impact on the theory.

We take

$$\mu(i^p z^q, n) = \begin{cases} n + p & \text{if } p \neq 0 \\ 0 & \text{if } n = p = 0 \\ \uparrow & \text{if } n \neq p = 0 \end{cases}$$

for all $n \in \mathbb{N}$. In particular, write $1 = i^0 z^0$. This defines a modification function. Note that i is the incrementation action whilst z says 'if zero then tick'.

Consider the processes E and F defined by

$$\begin{array}{ll} E = i : E' & E' = i : E + z : F \\ F = i : F' & F' = F \end{array}$$

using auxilliary processes E' and F'. These processes generate transition structures that look as follows:

$$n, E \xrightarrow{i} n + 1, E' \xrightarrow{i} n + 2, E \xrightarrow{i} \ldots$$

$$n, F \xrightarrow{i} n + 1, F' \xrightarrow{i} n + 2, F \xrightarrow{i} \ldots$$

starting from any n.

Now n, E and n, F have identical operational behaviour. Since $0, E'$ is unreachable, it is clear that

$$\forall n.\ n, E \sim_\mu n, F$$

holds. We also have $n+1, E' \sim_\mu n+1, F'$, for all n. However, $0, E'$ and $0, F'$ have distinct operational behaviour since we have $0, E' \xrightarrow{z} 0, E$ as a transition.

Consider an atomic ϕ such that and $n, G \vDash \phi$ if and only if $n = 0$ and G is 1, the unit process. Using the semantic clauses for $-\!\!*$ and $\langle - \rangle$, we can verify that $1, E' \vDash \phi -\!\!* \langle z \rangle \top$ and $1, F' \nvDash \phi -\!\!* \langle z \rangle \top$ since only $0, 1 \vDash \phi$ and $1, 1 \times E' \xrightarrow{z} 1, 1 \times E \vDash \top$ but $0, 1 \times F'$ makes no z-transition. We therefore have that

$$0, E \vDash \langle i \rangle (\phi -\!\!* \langle z \rangle \top) \qquad 0, F \nvDash \langle i \rangle (\phi -\!\!* \langle z \rangle \top)$$

hold.

This tells us that Theorem 9.1 of [PT06] fails as stated in the presence of both $\langle - \rangle$ and $-\!\!*$. It also tells us that the operational equivalence $\sim_\mu$ is not contained in (or equal to) the logical equivalence relation.

2. Corrections to HPL-2004-170R2

We must amend Definition 1, and make the necessary consequent amendments. The significance of the amendment is explained in § 5.

Definition 1, page 10, should be stated as follows:

Bisimulation, $\sim_\mu$, is the largest binary relation on processes E such that if $E \sim_\mu F$, then

(i) for all R, $R, E \xrightarrow{a} \mu(a, R), E'$ implies, for some F',
$$R, F \xrightarrow{a} \mu(a, R), F' \text{ and } E' \sim_\mu F', \text{ and}$$

(ii) for all R, $R, F \xrightarrow{a} \mu(a, R), F'$ implies, for some E',
$$R, E \xrightarrow{a} \mu(a, R), E' \text{ and } E' \sim_\mu F'.$$

We refer to this bisimulation as *global* bisimulation.

For Theorem 9.2, however, we need the original definition of bisimulation. We use the symbol $\approx_\mu$ instead of $\sim_\mu$, and call it *local* bisimulation, to avoid confusion, as follows:

Local bisimulation, $\approx_\mu$, is the largest binary relation on resource–process pairs R, E such that if $R, E \sim_\mu R, F$, then

(i) $R, E \xrightarrow{a} \mu(a, R), E'$ implies, for some F',
$$R, F \xrightarrow{a} \mu(a, R), F' \text{ and } \mu(a, R), E' \approx_\mu \mu(a, R), F', \text{ and}$$

(ii) $R, F \xrightarrow{a} \mu(a, R), F'$ implies, for some E',
$$R, E \xrightarrow{a} \mu(a, R), E' \text{ and } \mu(a, R), E' \approx_\mu \mu(a, R), F'.$$

The appropriate notion of congruence for this equivalence is then the following: if, for all R, $R, E \approx_\mu R, F$, then, for all evident terms, a, X, G, R, and S, we have $R, a : E \approx_\mu R, a : F$, $R, E + G \approx_\mu R, F + G$, $R, E \times G \approx_\mu R, F \times G$, and $R, (\nu S)E \approx_\mu R, (\nu S)F$.

This definition of local bisimulation should be inserted at the end of § 4.

The following amendments then arise as consequences:

- All assertions of the form $R, E \sim_\mu R, F$ should be replaced by the corresponding $E \sim_\mu F$ *except those in Theorem 9.2*;
- Theorem 9.1, p. 22, should be: '*If* $E \sim_\mu F$*, then, for all* R*, it follows that* $R, E \equiv_{\mathbf{MBI}} R, F$*.*';
- The first sentence of the paragraph immediately before Theorem 9.2 should be: 'It follows that, for image-finite processes, the argument of Stirling [Sti01] can be applied rather straightforwardly provided we use the local bisimulation, $\approx_\mu$, including for the definition of the logical connectives as given in Table 2.';
- Theorem 9.2, p. 24, should be: 'If, for all R, R, E and R, F are image-finite and if, for all R, it is the case that $R, E \equiv_{\mathbf{MBI}} R, F$, then $E \approx_\mu F$.'

Known typographical errors:

- p. 18, l. -20: '$R \sqsubseteq e$' should be '$e \sqsubseteq R$';
- p. 23, l. 1: '$R \sqsubseteq e$' should be '$e \sqsubseteq R$';
- p. 24, l. -17: 'R' should be '$\mu(a, R)$';
- p. 24, l. -16: 'H' should be 'H_i';
- p. 27: In [BT00a], '3:281–305' should be '8(6–7):377–393, 2001';
- p. 27: In [BT00b], '3:281–305' should be '8(6–7):395–414, 2001'.

3. Corrections to *Formal Aspects of Computing* (2006) 18:495–517, [PT06]

We must amend Definition 1, and make the necessary consequent amendments. The significance of the amendment is explained in § 5.

Definition 1, page 502, should be stated as follows:

Bisimulation, $\sim_\mu$, is the largest binary relation on processes E such that if $E \sim_\mu F$, then

(i) for all R, $R, E \xrightarrow{a} \mu(a, R), E'$ implies, for some F',

$$R, F \xrightarrow{a} \mu(a, R), F' \text{ and } E' \sim_\mu F', \text{ and}$$

(ii) for all R, $R, F \xrightarrow{a} \mu(a, R), F'$ implies, for some E',

$$R, E \xrightarrow{a} \mu(a, R), E' \text{ and } E' \sim_\mu F'.$$

We refer to this bisimulation as *global* bisimulation.

For Theorem 9.2, however, we need the original definition of bisimulation. We use the symbol $\approx_\mu$ instead of $\sim_\mu$, and call it *local* bisimulation, to avoid confusion, as follows:

Local bisimulation, $\approx_\mu$, is the largest binary relation on resource–process pairs R, E such that if $R, E \sim_\mu R, F$, then

(i) $R, E \xrightarrow{a} \mu(a, R), E'$ implies, for some F',

$$R, F \xrightarrow{a} \mu(a, R), F' \text{ and } \mu(a, R), E' \approx_\mu \mu(a, R), F', \text{ and}$$

(ii) $R, F \xrightarrow{a} \mu(a, R), F'$ implies, for some E',

$$R, E \xrightarrow{a} \mu(a, R), E' \text{ and } \mu(a, R), E' \approx_\mu \mu(a, R), F'.$$

The appropriate notion of congruence for this equivalence is then the following: if, for all R, $R, E \approx_\mu R, F$, then, for all evident terms, a, X, G, R, and S, we

have $R, a : E \approx_\mu R, a : F$, $R, E + G \approx_\mu R, F + G$, $R, E \times G \approx_\mu R, F \times G$, and $R, (\nu S)E \approx_\mu R, (\nu S)F$.

This definition of local bisimulation should be inserted at the end of § 4.

The following amendments then arise as consequences:

- All assertions of the form $R, E \sim_\mu R, F$ should be replaced by the corresponding $E \sim_\mu F$ *except those in Theorem 9.2*;
- Theorem 9.1, p. 512, should be: '*If* $E \sim_\mu F$*, then, for all* R*, it follows that* $R, E \equiv_{\mathbf{MBI}} R, F$.';
- The first sentence of the paragraph immediately before Theorem 9.2 should be: 'It follows that, for image-finite processes, the argument of Stirling [Sti01] can be applied rather straightforwardly provided we use the local bisimulation, $\approx_\mu$, including for the definition of the logical connectives as given in Table 2.';
- Theorem 9.2, p. 513, should be: 'If, for all R, R, E and R, F are image-finite and if, for all R, it is the case that $R, E \equiv_{\mathbf{MBI}} R, F$, then $E \approx_\mu F$.'

Known typographical errors:

- p. 509, l. -19: '$R \sqsubseteq e$' should be '$e \sqsubseteq R$';
- p. 513, l. 6: '$R \sqsubseteq e$' should be '$e \sqsubseteq R$';
- p. 514, l. 12: 'R' should be '$\mu(a, R)$';
- p. 514, l. 13: 'H' should be 'H_i';
- p. 516: In [BT00a], '3:281–305' should be '8(6–7):377–393, 2001';
- p. 516: In [BT00b], '3:281–305' should be '8(6–7):395–414, 2001'.

4. Consequences for the paper *Electronic Notes in Theoretical Computer Science* 172, 545–587, 2007, [PT07]

In all sections *except* § 5, we need to make the same amendments as for [PT06]. Specifically:

Definition 3.1, p. 555, should be stated as follows:
Bisimulation, $\sim_\mu$, is the largest binary relation on processes E such that if $E \sim_\mu F$, then

(i) for all R, $R, E \xrightarrow{a} \mu(a, R), E'$ implies, for some F',

$$R, F \xrightarrow{a} \mu(a, R), F' \text{ and } E' \sim_\mu F', \text{ and}$$

(ii) for all R, $R, F \xrightarrow{a} \mu(a, R), F'$ implies, for some E',

$$R, E \xrightarrow{a} \mu(a, R), E' \text{ and } E' \sim_\mu F'.$$

For § 5 and for Theorems 8.3 and 9.2, however, we need the original bisimulation. We use the symbol $\approx_\mu$ instead of $\sim_\mu$, and call it *local* bisimulation, to avoid confusion, as follows:

Local bisimulation, $\approx_\mu$, is the largest binary relation on resource–process pairs R, E such that if $R, E \sim_\mu R, F$, then

(i) $R, E \xrightarrow{a} \mu(a, R), E'$ implies, for some F',

$$R, F \xrightarrow{a} \mu(a, R), F' \text{ and } \mu(a, R), E' \approx_\mu \mu(a, R), F', \text{ and}$$

(ii) $R, F \xrightarrow{a} \mu(a, R), F'$ implies, for some E',

$$R, E \xrightarrow{a} \mu(a, R), E' \text{ and } \mu(a, R), E' \approx_\mu \mu(a, R), F'.$$

The appropriate notion of congruence for this equivalence is then the following: if, for all R, $R, E \approx_\mu R, F$, then, for all evident terms, a, X, G, R, and S, we have $R, a : E \approx_\mu R, a : F$, $R, E + G \approx_\mu R, F + G$, $R, E \times G \approx_\mu R, F \times G$, $R, (\nu S)E \approx_\mu R, (\nu S)F$, and $R, \mathrm{fix}X.E \approx_\mu R, \mathrm{fix}X.F$.

This definition of local bisimulation should be inserted at the end of § 3.

The following amendments then arise as consequences:

- In § 5: Each occurence of '$\sim_\mu$' should be '$\approx_\mu$';
- All assertions of the form $R, E \sim_\mu R, F$ should be replaced by the corresponding $E \sim_\mu F$, *except in § 5 and in Theorem 8.3 and its immediately preceding paragraph*;
- Theorem 8.2, p. 575, should be: '*If $E \sim_\mu F$, then, for all R, it follows that $R, E \equiv_{\mathbf{MBI}} R, F$.*';
- p. 577, l. -4: '$\sim_\mu$' should be '$\approx_\mu$';
- p. 577, l. -3: The sentence beginning 'For now, ... ' should be: 'For now, however, we establish the basic result for image-finite processes, with the argument following that of Stirling [Sti01] rather straightforwardly provided we use the local bisimulation, $\approx_\mu$, including for the definition of the logical connectives as given in Table 5.';
- Theorem 8.3, p. 578, should be: 'If, for all R, R, E and R, F are image-finite and if, for all R, it is the case that $R, E \equiv_{\mathbf{MBI}} R, F$, then $E \approx_\mu F$.'

The extensions of Theorems 8.2 and 8.3 given in § 9, namely Theorems 9.1 and 9.2 require corresponding amendments.

- Theorem 9.1. p. 580, should be: 'For all R, if $E \sim_\mu F$, then $R, E \equiv_{\mathbf{MBI}} R, F$.'
- Theorem 9.2, p. 580, should be: 'Let R, E and R, F be image-finite. If, for all R, $R, E \equiv_{\mathbf{MBI}} R, F$, then $E \approx_\mu F$.'

The significance of these amendments is explained in § 5.

Finally, the following typographical corrections are known:

- p. 572, l. -21: '$R \sqsubseteq e$' should be '$e \sqsubseteq R$';
- p. 576, l. -15: '$R \sqsubseteq e$' should be '$e \sqsubseteq R$';
- p. 578, l. -13: 'R' should be '$\mu(a, R)$'.

5. Discussion

Our (non-typographical) corrections are all based on the necessary correction to the definition of bisimulation required for the logical equivalence theorems to hold (for the full **MBI** logic). Notice, however, that our original definition of bisimulation is the correct one for our denotational semantics, given in § 5 of [PT07], which corresponds to the operational behaviour of **SCRP**.

So, there is a mismatch between between the operational behaviour of **SCRP** and the logical strength of full **MBI**. In particular, as we have seen in § 1, a mismatch occurs when $-\!\!*$ and $\langle - \rangle$ are both present in the logic. There exist fragments of **MBI**, however, for which the logical equivalence theorems hold for both $\sim_\mu$ and $\approx_\mu$: for example, **MBI** without $-\!\!*$ and the multiplicative quantifiers and modalities but, importantly, with $*$ and the additive modalities. Indeed, such fragments appear to be useful in practical modelling work.

Notice that we have renamed the original notion of bisimulation, now denoted $\approx_\mu$, as 'local'. This is in contrast to the 'global' form required for (one direction

of) the logical equivalence result. For instance, in the example of § 1, the local equivalence is available but the global one is not, so that logical equivalence fails. The local equivalence holds because the states $0, E'$ and $0, F'$ are not reachable in the transition system and the global one fails because the quantification over all resources includes 0.

The mismatch shows that the expressivity of **MBI** exceeds that which is captured by the local equivalence. In particular, again referring to the example of § 1, the local equivalence fails to distinguish the perturbations, $0, E'$ and $0, F'$, of $1, E'$ and $1, F'$ (which are not logically equivalent). The global equivalence distinguishes such perturbations.

Finding a bisimulation that yields both the logical equivalence theorem for full **MBI** and an internal full abstraction theorem, so that we might obtain an appropriate account of 'domain theory in logical form' in our setting, appears to be a challenging problem.

References

[PT06] David Pym and Chris Tofts. A calculus and logic of resources and processes. *Formal Aspects of Computing*, 18(4):495–517, 2006.

[PT07] David Pym and Chris Tofts. Systems Modelling via Resources and Processes: Philosophy, Calculus, Semantics, and Logic. In L. Cardelli, M. Fiore, and G. Winskel, editors, *Electronic Notes in Theoretical Computer Science (Computation, Meaning, and Logic: Articles dedicated to Gordon Plotkin)*, volume 107, pages 545–587, 2007.

HP Labs, Bristol
E-mail address: matthew.collinson@hp.com

HP Labs, Bristol, UK
E-mail address: david.pym@hp.com

HP Labs, Bristol, UK
E-mail address: chris.tofts@hp.com